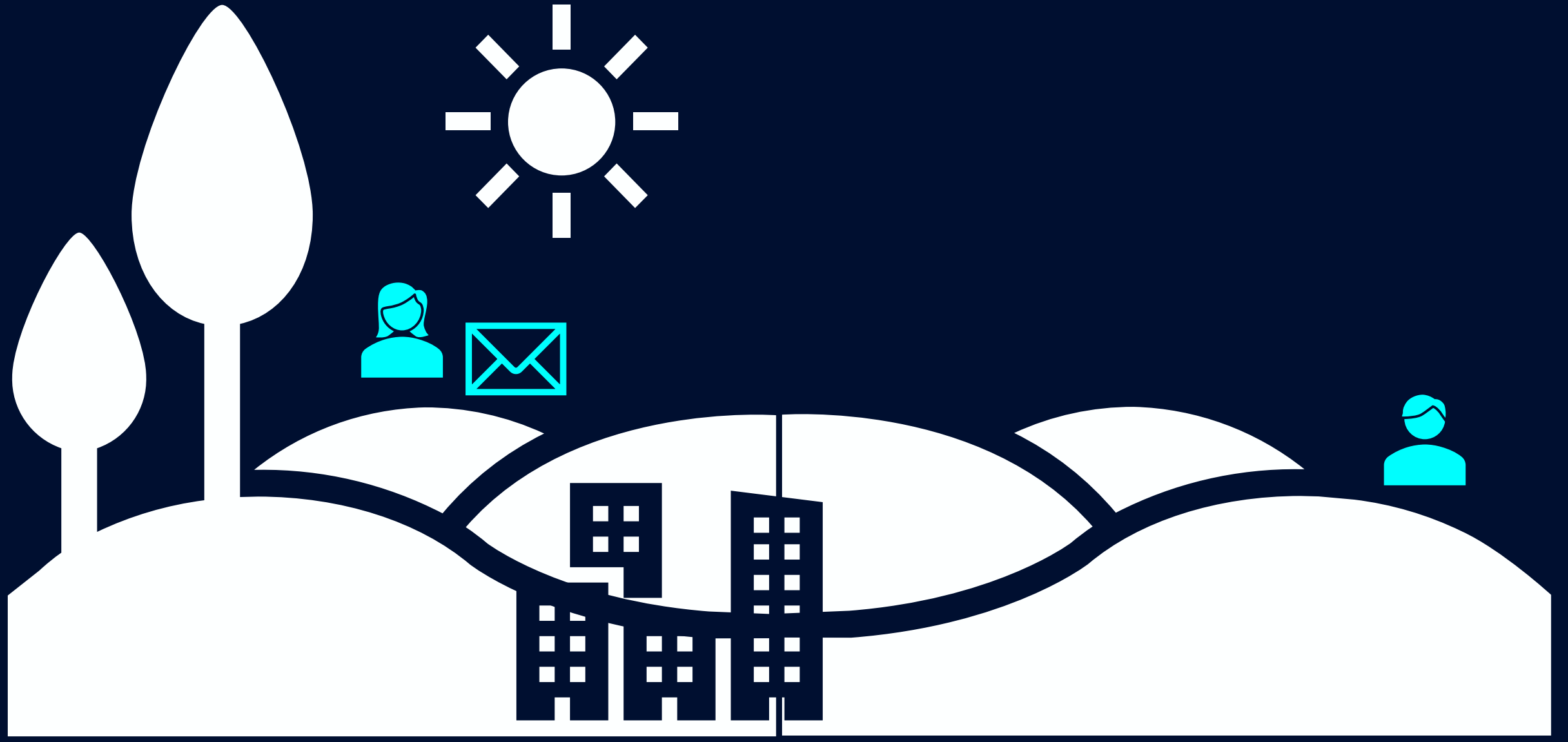
Cracking the codes of Alice

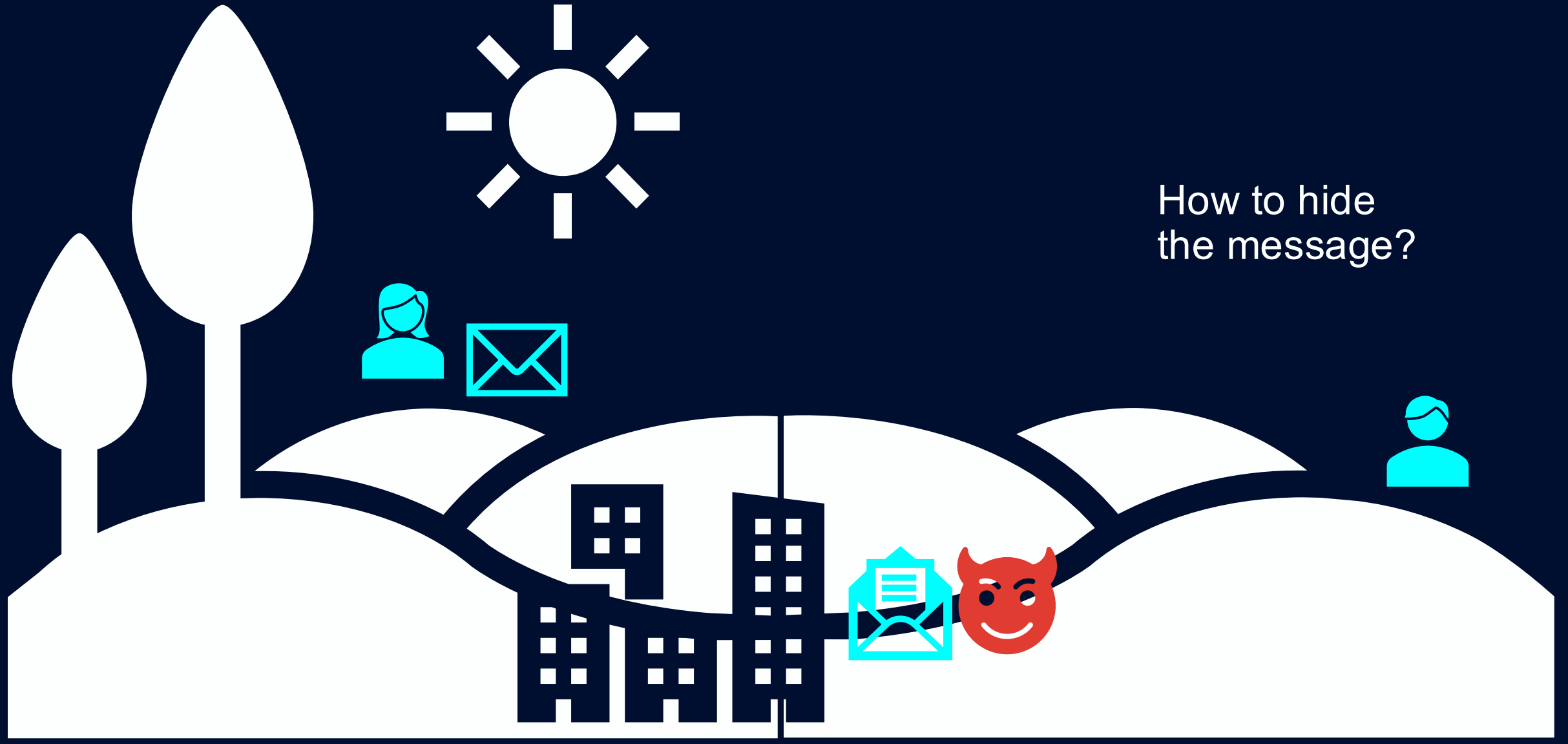
Tjitske Koster | PhD at TU Delft

2-3-2026

Alice and Bob



Eve



How to hide
the message?

Tjitske Koster

TU Delft

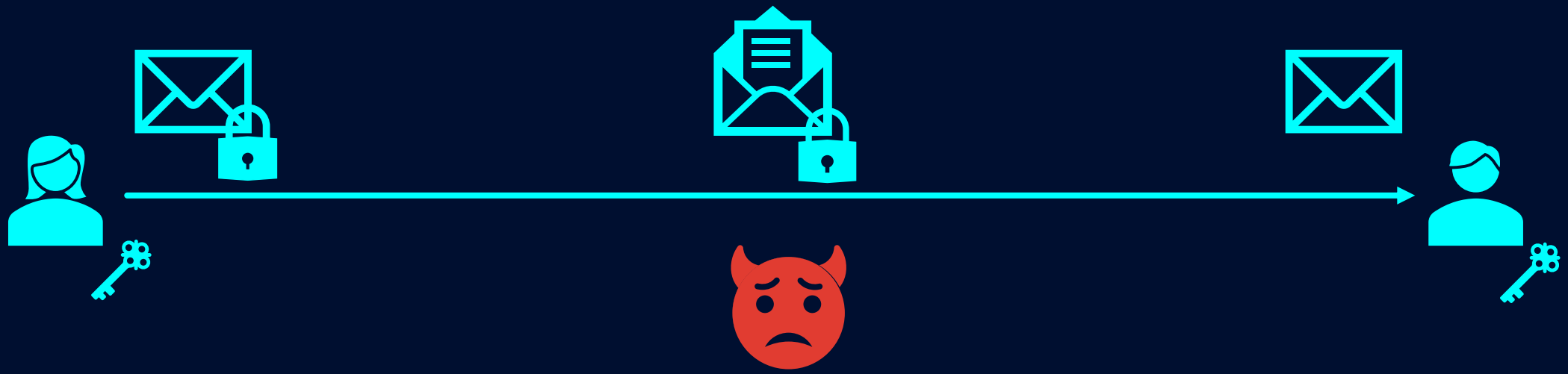
Librae

Goal today

- Introduce the endless battle of cryptography

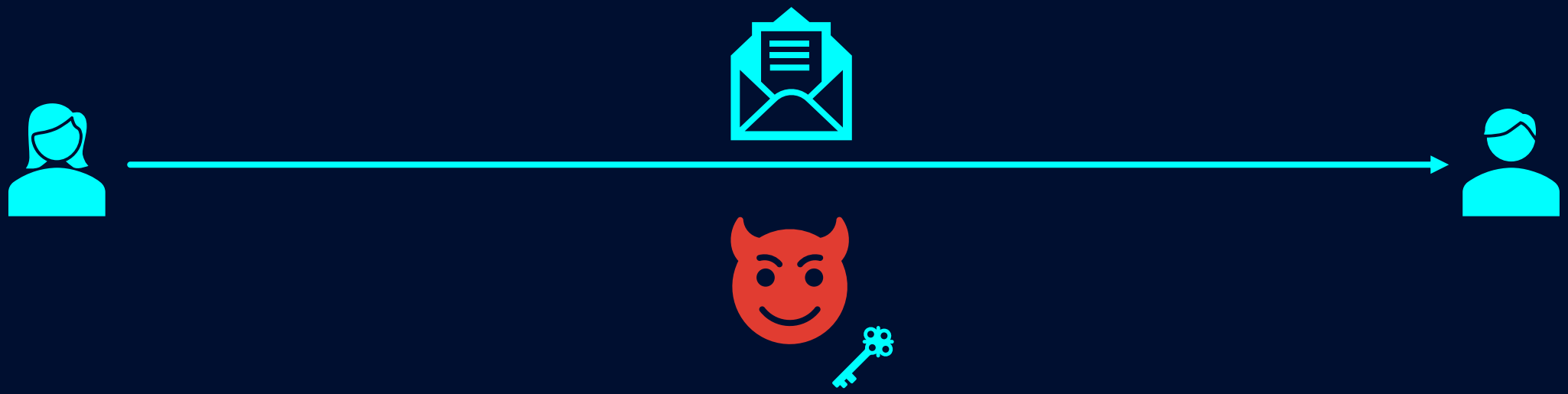
Goal of Alice

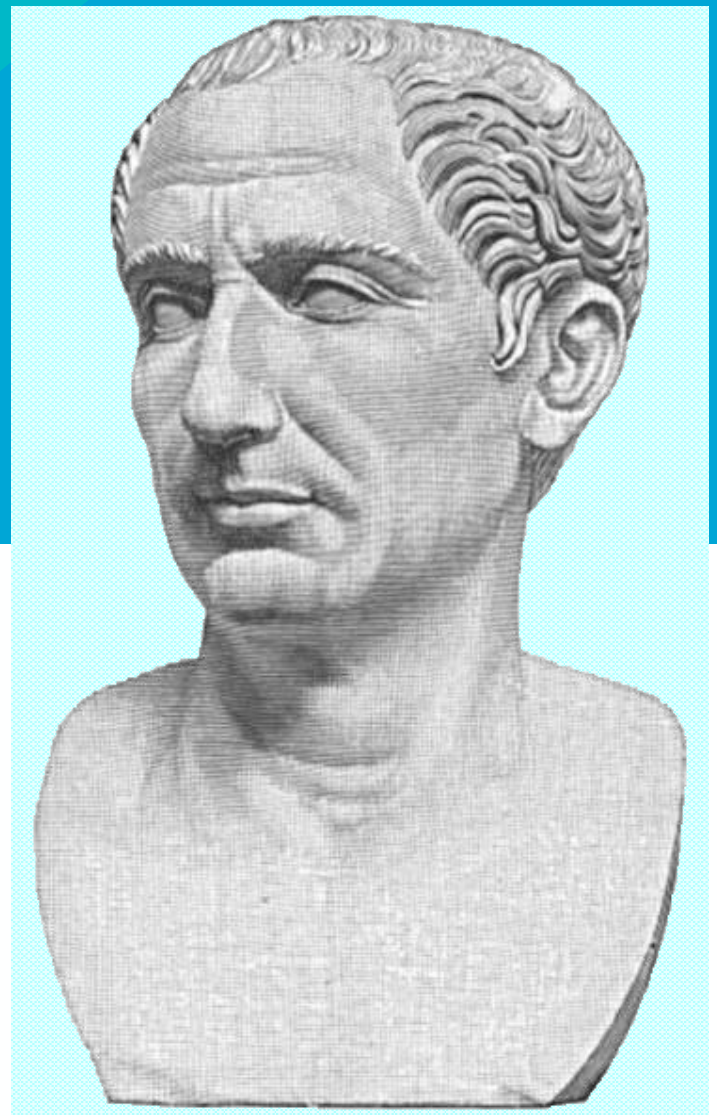
- A code that only Alice and Bob know
- Alice can *Encrypt* the message Ciphertext
- Bob can *Decrypt* the message Plaintext
- If Eve sees the message, she will not understand



Goal of Eve (us)

- Break the code of Alice



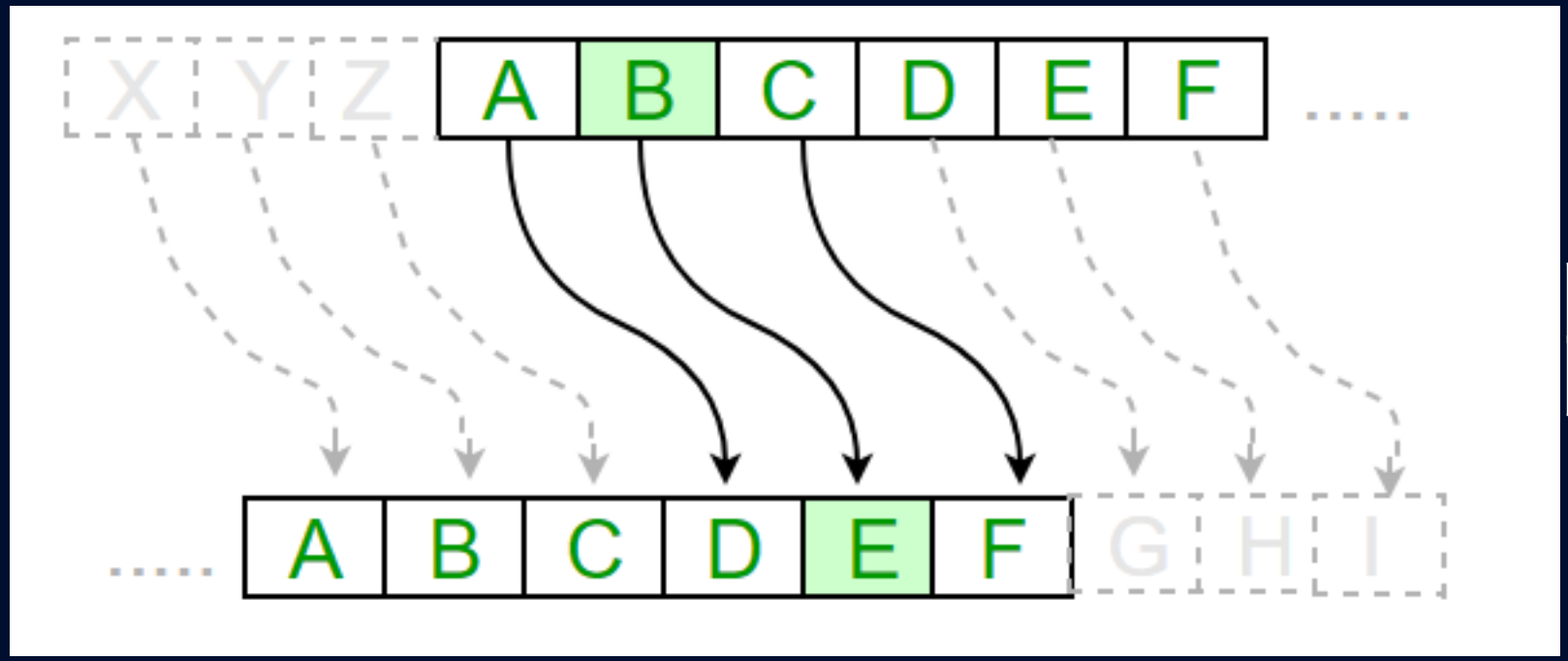


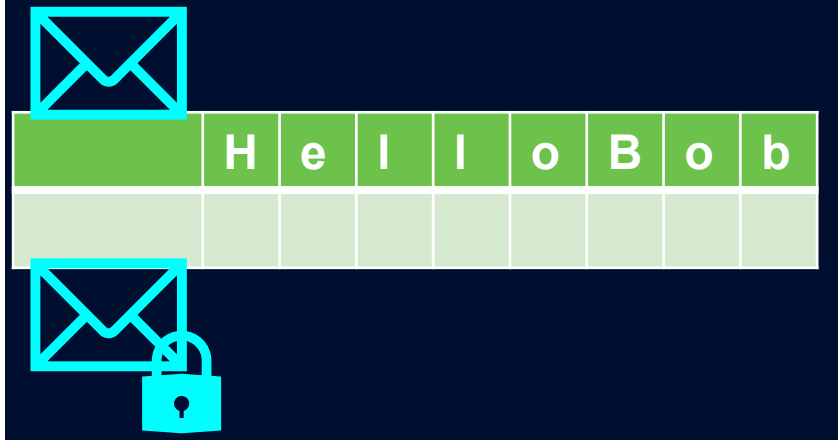
Caesar cipher

50 BC

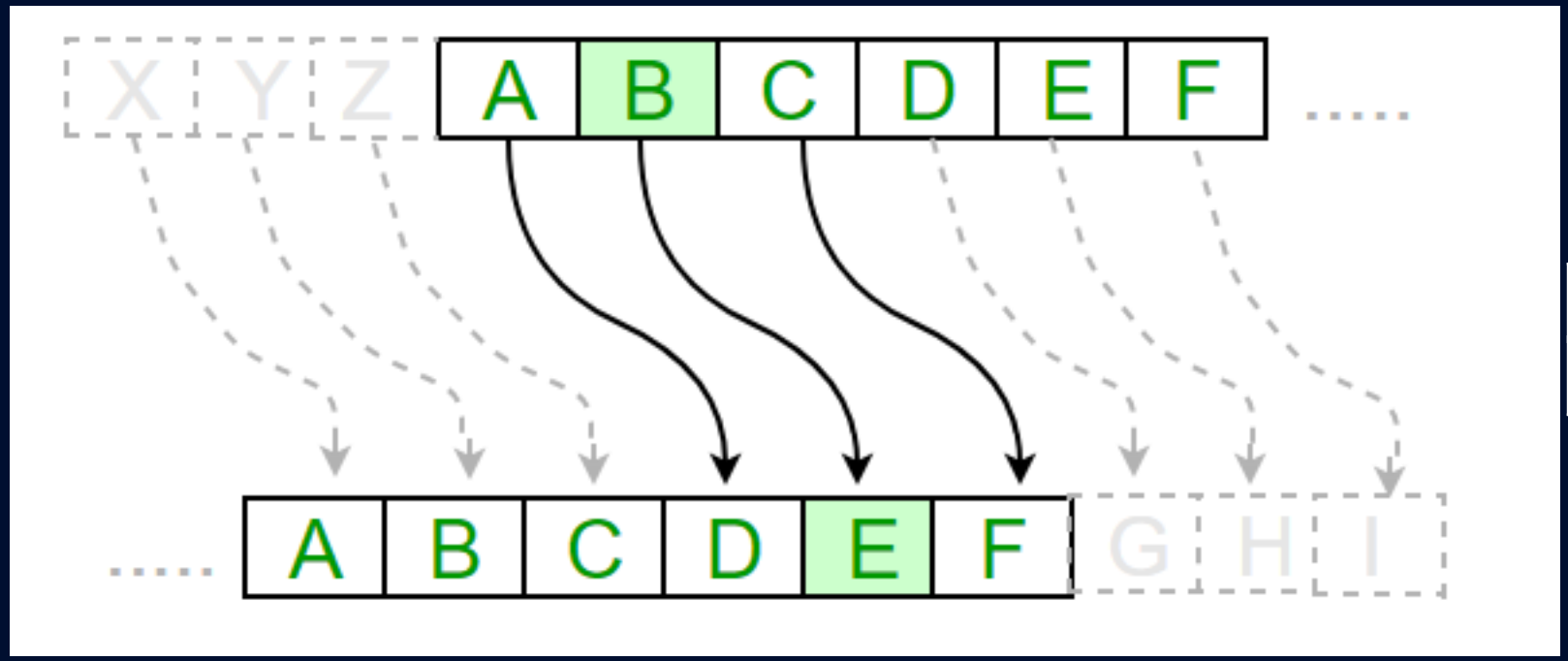
The first encryption Caesar Cipher

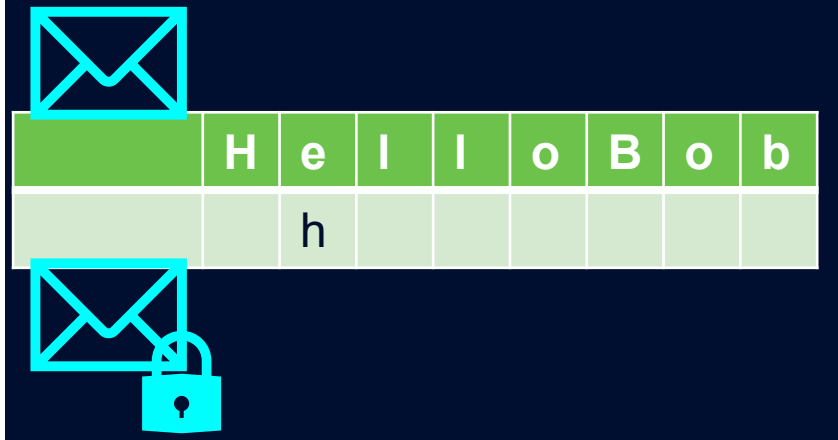
- Replace each letter with a letter K places further in the alphabet



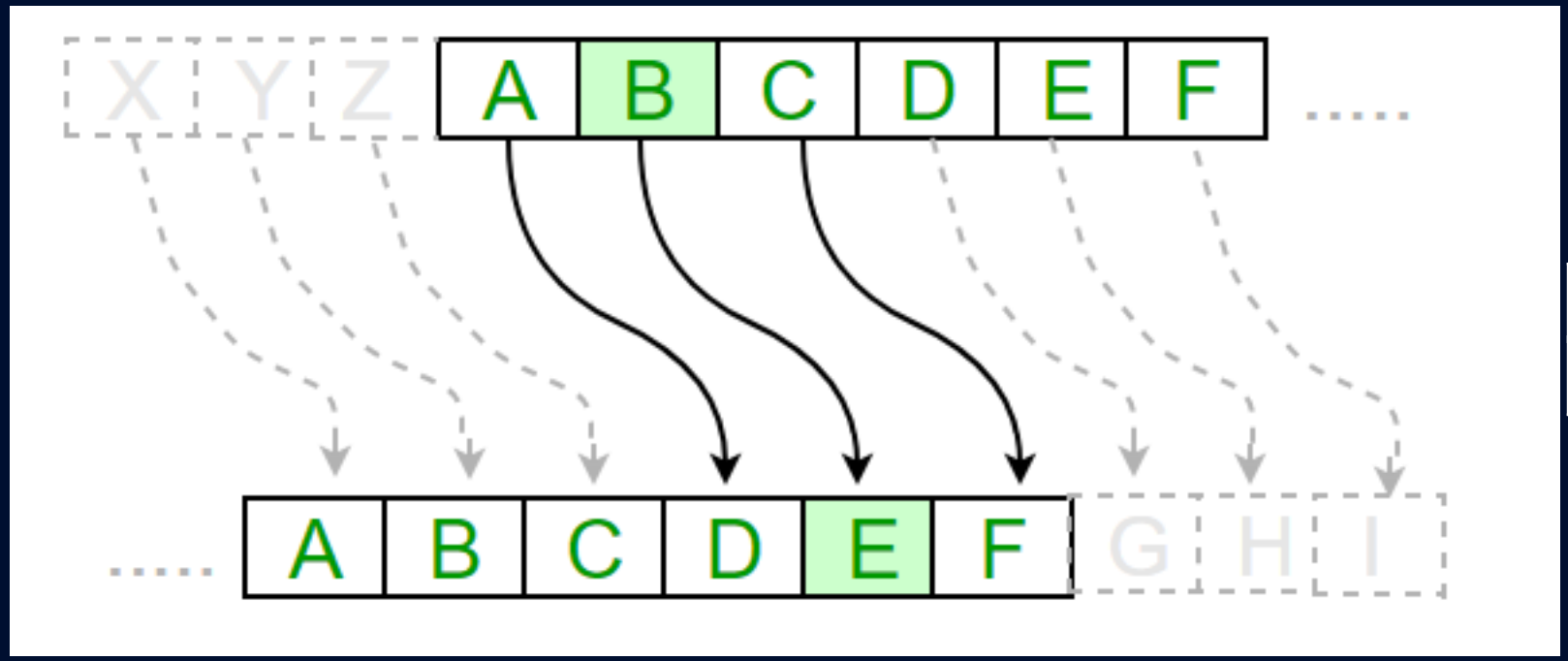


The first encryption Caesar Cipher





The first encryption Caesar Cipher



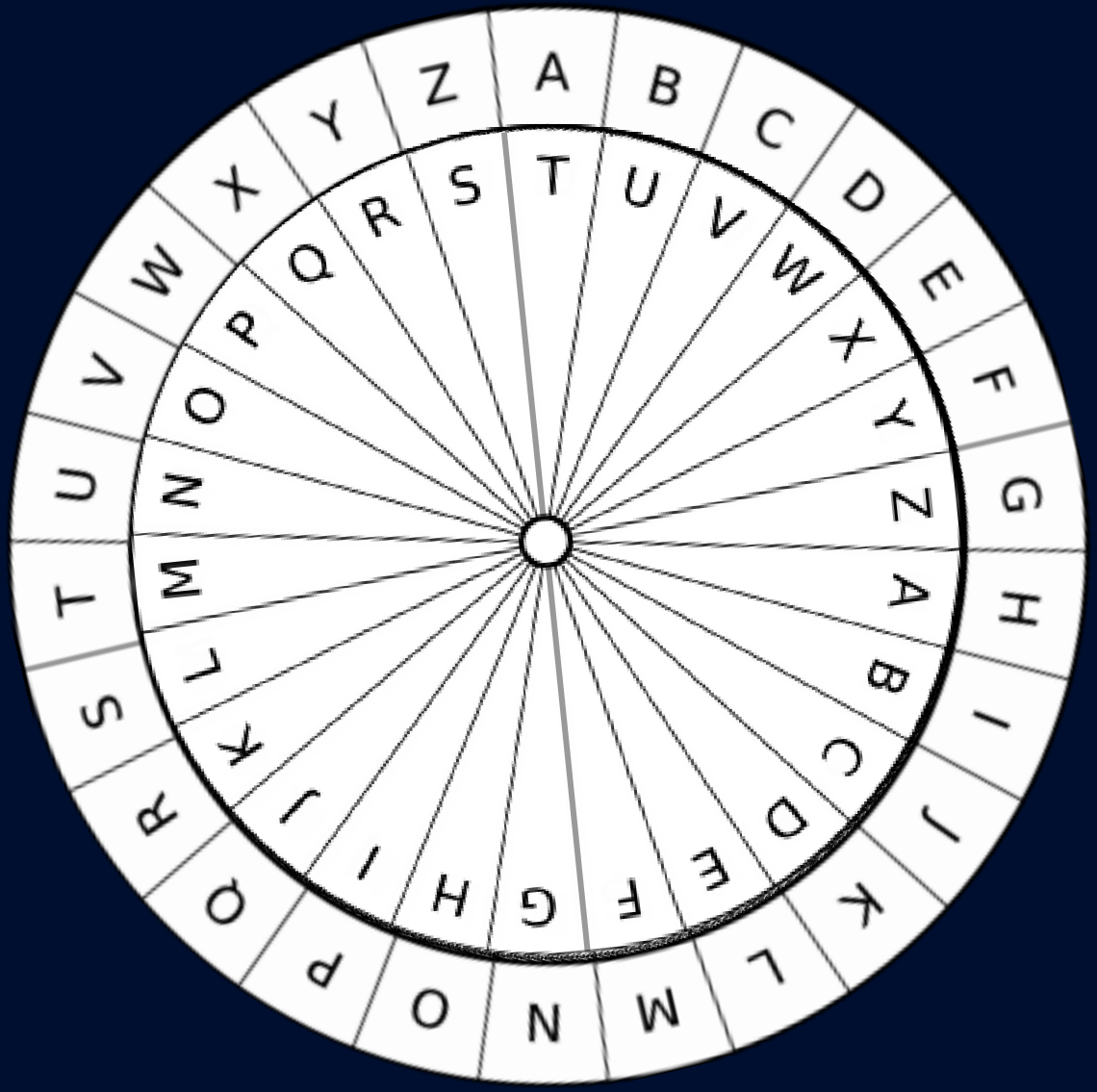
	H	e	l	l	o	B	o	b
	K	h	o	o	r	E	r	e

Breaking Caesar

Olssv ivi!

Breaking Caesar

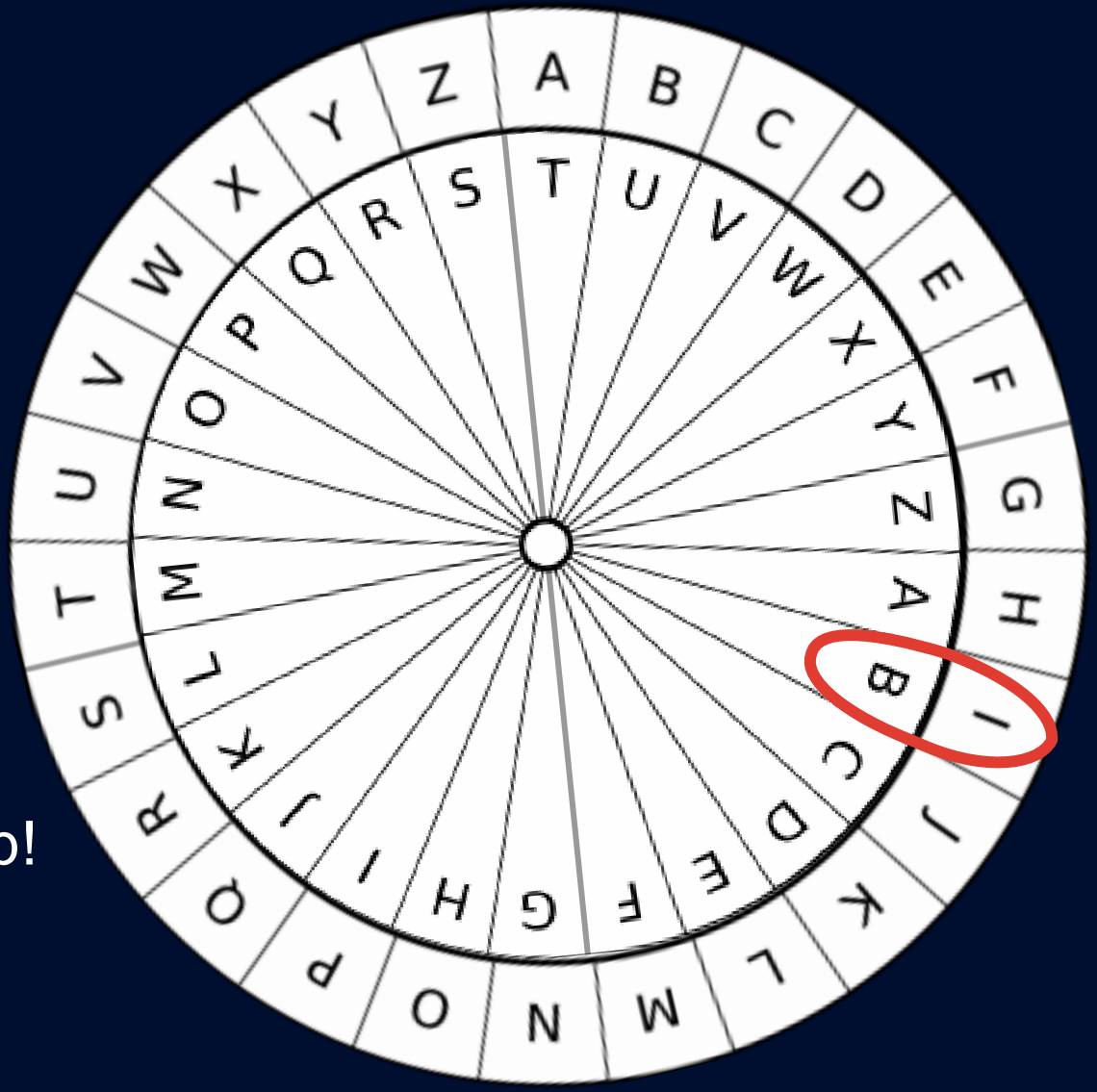
Olssv ivi!



Breaking Caesar

Olssv ivi!

Hello Bob!



Linguistic analysis

Uvd kbypun aopz aptl Zohoyhghk ohk ivyul rpun Zohoypfhy aoyll zvuz. Vu aol aovbzhuk huk mpyza upnoa, dolu zol ohk luklk aol ahsl vm Th'hybm, zol yvzl huk rpzzlk aol nyvbuk ilmvyl opt, zhfpun: “nylha rpun, mvy h aovbzhuk huk vul upnoaz P ohcl illu yljvbuapun av fvb aol mhislz vm whza hnlz huk aol slnlukz vm hujplua rpunz. Thf P thrl zv ivsk hz av jyhcl h mhcvby vm fvby thqlzaf?”
Lwpsvnbl, Ahslz myvt aol Aovbzhuk huk Vul Upnoaz

Linguistic analysis

Uvd kbypun aopz aptl Zohoyhghk ohk ivyul rpun Zohoypfhy aoyll zvuz. Vu aol aovbzhuk huk mpyza upnoa, dolu zol ohk luklk aol ahsl vm Th'hybm, zol yvzl huk rpzzlk aol nyvbuk ilmvyl opt, zhfpun: “nylha rpun, mvy h aovbzhuk huk vul upnoaz P ohcl illu yljvbuapun av fvb aol mhislz vm whza hnlz huk aol slnlukz vm hujplua rpunz. Thf P thrl zv ivsk hz av jyhcl h mhcvby vm fvby thqlzaf?”
Lwpsvnbl, Ahslz myvt aol Aovbzhuk huk Vul Upnoaz

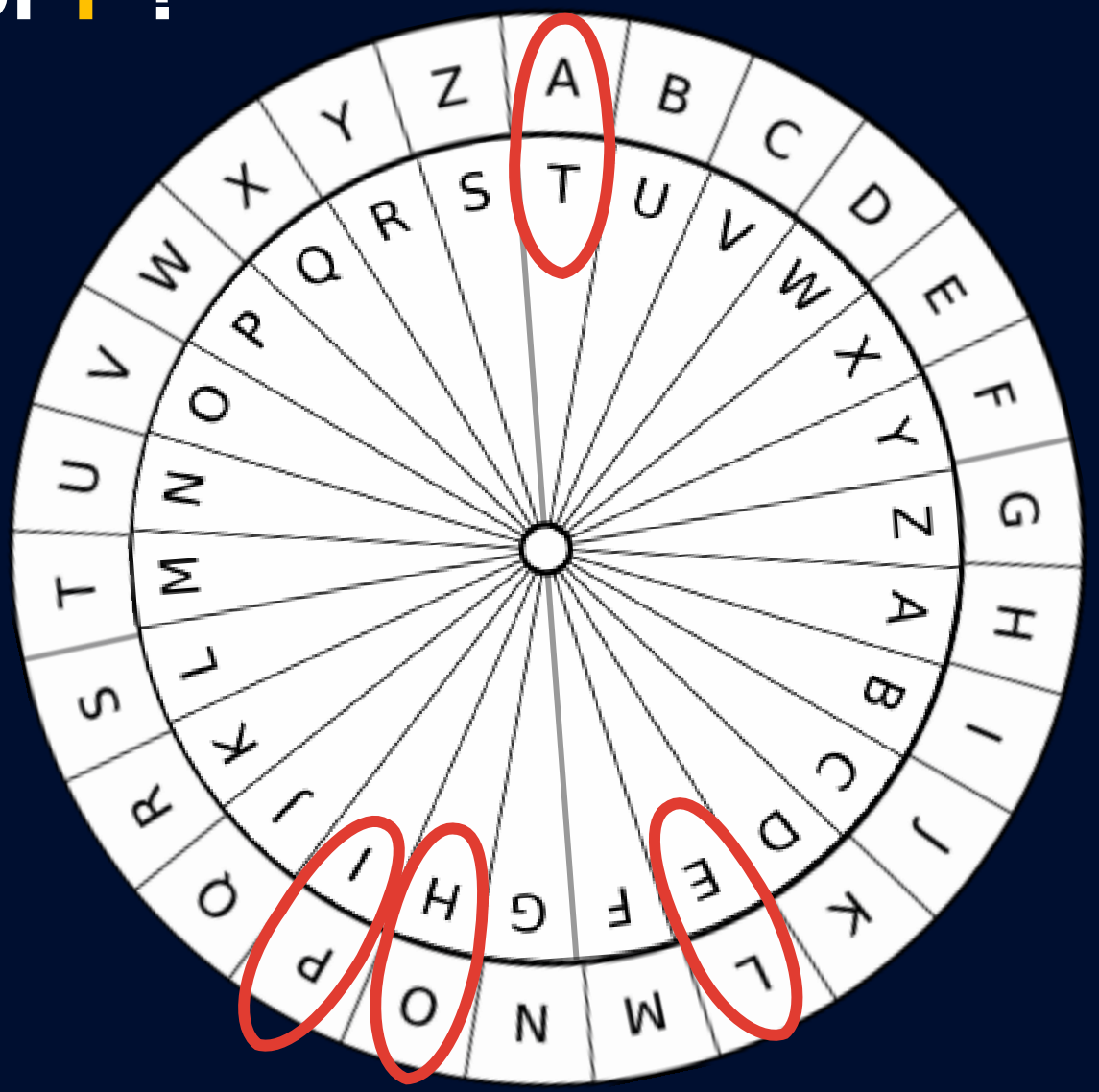
Linguistic analysis

Uvd kbypun aopz aptl Zohoyhghk ohk ivyul rpun Zohoypfhy aoyll zvuz. Vu aol aovbzhuk huk mpyza upnoa, dolu zol ohk luklk aol ahsl vm Th'hybm, zol yvzl huk rpzzlk aol nyvbuk ilmvyl opt, zhfpun: “nylha rpun, mvy h aovbzhuk huk vul upnoaz P ohcl illu yljvbuapun av fvb aol mhislz vm whza hnlz huk aol slnlukz vm hujplua rpunz. Thf P thrl zv ivsk hz av jyhcl h mhcvby vm fvby thqlzaf?”
Lwpsvnbl, Ahslz myvt aol Aovbzhuk huk Vul Upnoaz

What would aol be, or P?

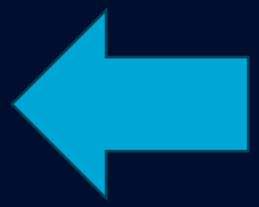
- aol → the ?
- P → I?

- A → T
- O → H
- L → E
- P → I



Linguistic analysis - Decryption

Now during this time Shahrazad had borne king Shahriyar three sons. On the thousand and first night, when she had ended the tale of Ma'aruf, she rose and kissed the ground before him, saying: “great king, for a thousand and one nights I have been recounting to you the fables of past ages and the legends of ancient kings. May I make so bold as to crave a favour of your majesty?”
Epilogue, Tales from the Thousand and One Nights



Uvd kbypun aopz aptl Zohoyhghk ohk ivyul rpun Zohoypfhy aoyll zvuz. Vu aol aovbzhuk huk mpyza upnoa, dolu zol ohk luklk aol ahsl vm Th'hybm, zol yvzl huk rpzzlk aol nyvbuk ilmvyl opt, zhfpun: “nylha rpun, mvy h aovbzhuk huk vul upnoaz P ohcl illu yljvbuapun av fvb aol mhislz vm whza hnlz huk aol slnlukz vm hujplua rpunz. Thf P thrl zv ivsk hz av jyhcl h mhcvby vm fvby thqlzaf?”
Lwpsvnbl, Ahslz myvt aol Aovbzhuk huk Vul Upnoaz

What went wrong?

- Spaces
- Capitals
- Punctuation

- Only 25 encryptions possible; brute force attack is feasible

Vigenère cipher

16th century

The second encryption  Vigenère 

- We assign numbers to each letter

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9

K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19

U	V	W	X	Y	Z
20	21	22	23	24	25

The second encryption  Vigenère 

- Alice and bob agree on a secret: **KEY**
- Alice translate message to numbers
- Alice writes the secret
- Alice translate secret to numbers
- Alice adds the message to the secret
- Alice translate numbers to letters

H	E	L	L	O	B	O	B
07	04	11	11	14	01	14	01
K	E	Y	K	E	Y	K	E
10	04	24	10	04	24	10	04
17	8	9	21	18	25	24	05
R	I	J	V	S	Z	Y	F

7 + 10 =17

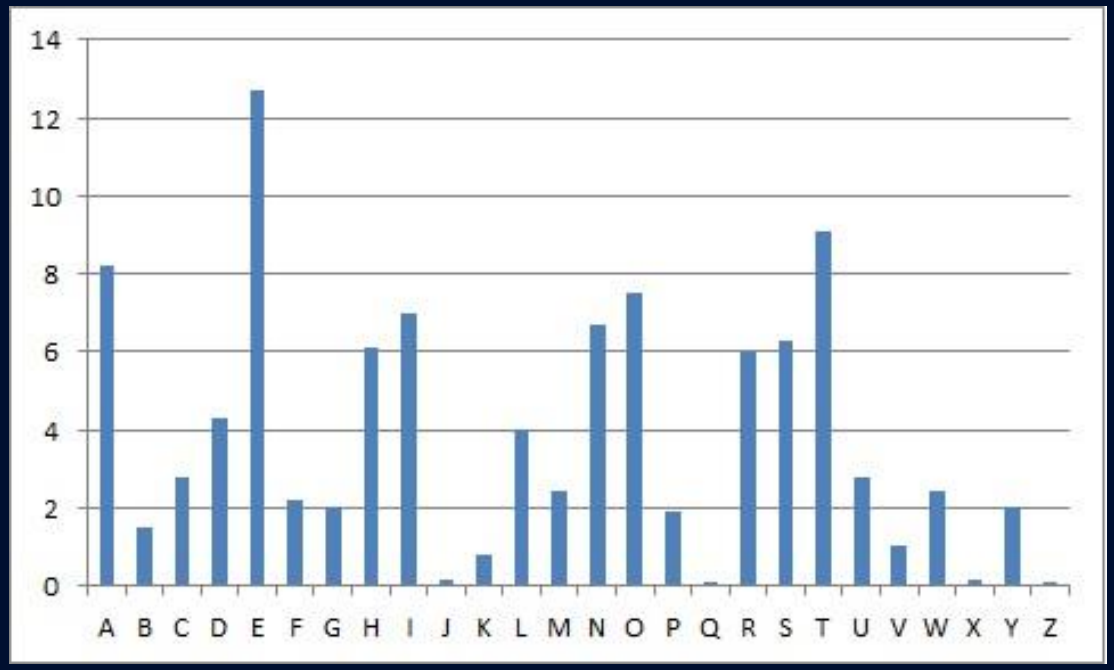
4 + 4 = 8

11+24 = 35 mod 26 = 9

Breaking Vigenère

- Frequency analysis
  - FACT: the most frequent letter in English: E

1. First, guess the length of the key
2. Second, count frequency
3. Third, guess the most frequent letter = E
4. Last, decrypt



Frequency analysis -> Vigenère

1. We guess the length of the key is 3

xsu nyp sre dlg cxg wiq ref bex khf khz yvl oog xkq ref bmw kvr rvc owm xwm xxf oxf yyq krb krb pmp cxl skf daf orq rif khc xhc nxf oxy vim pqy kvs pwf ovm ciy xhi swq ohr rie bss xhz ojm bif sqq kcg xke biy dog xkd yvy dlm ewy xhy xhm xil skf dwg ret ofc orp ogm err sre dsw yyr rid kfj owm pty cxy qiq krb dlc vie orb csd kra sil dog xkq wew sqy uiq yfm vhy cxm mvy fiy pet yyp yjw yyp weh owr iin spm qyc dej owd bsk dlc dlm ewy xhy xhm xil skf dw

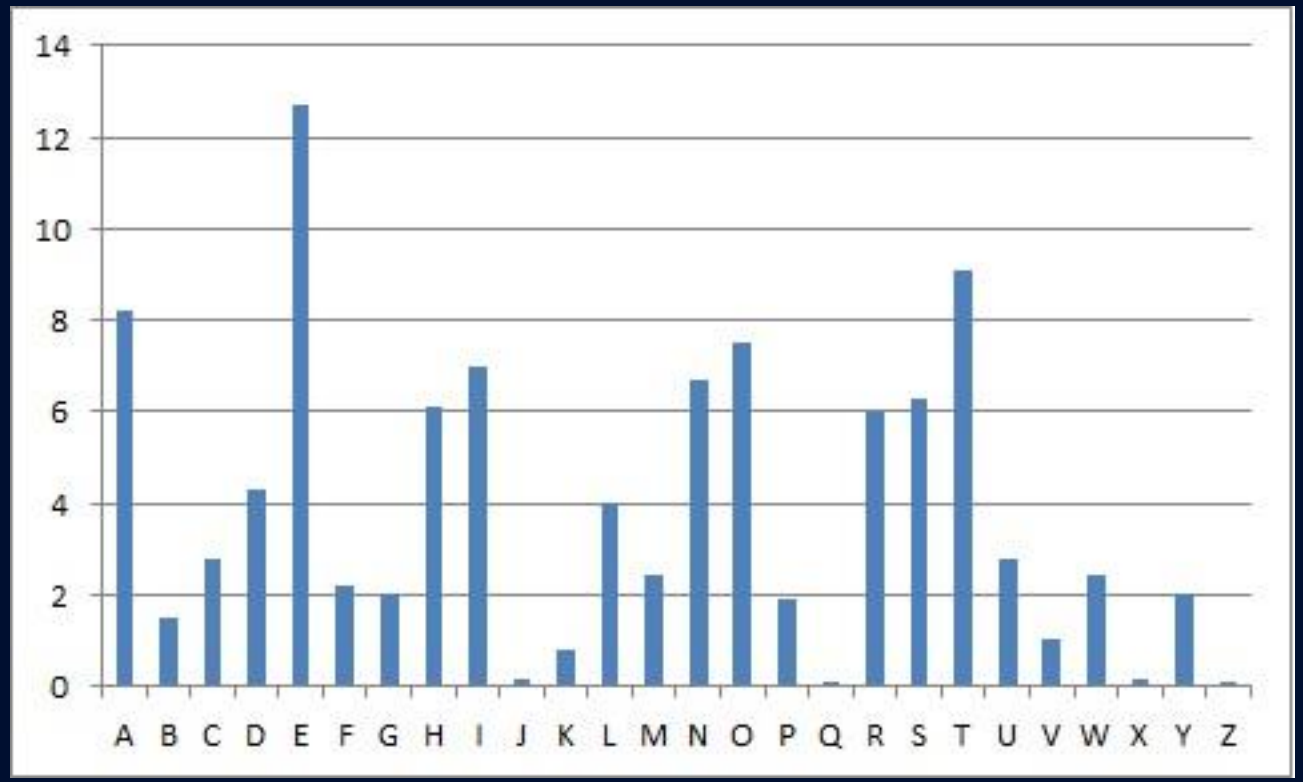
Frequency analysis -> Vigenère

1. We guess the length of the key is 3
2. We count the letters on the 1st 4th, 7th…. Spot
    1. Frequency O = 15
    2. Frequency D = 11
    3. Frequency K = 11

xsu nyp sre dlg cxg wiq ref bex khf
khz yvl oog xkq ref bmw kvr rvc
owm xwm xxf oxf yyq krb krb pmp
cxl skf daf orq rif khc xhc nxf oxy
vim pqy kvs pwf ovm ciy xhi swq ohr
rie bss xhz ojm bif sqq kcg xke biy
dog xkd yvy dlm ewy xhy xhm xil skf
dwg ret ofc orp ogm err sre dsw yyr
rid kfj owm pty cxy qiq krb dlc vie
orb csd kra sil dog xkq wew sqy uiq
yfm vhy cxm mvy fiy pet yyp yjw yyp
weh owr iin spm qyc dej owd bsk
dlc dlm ewy xhy xhm xil skf dw

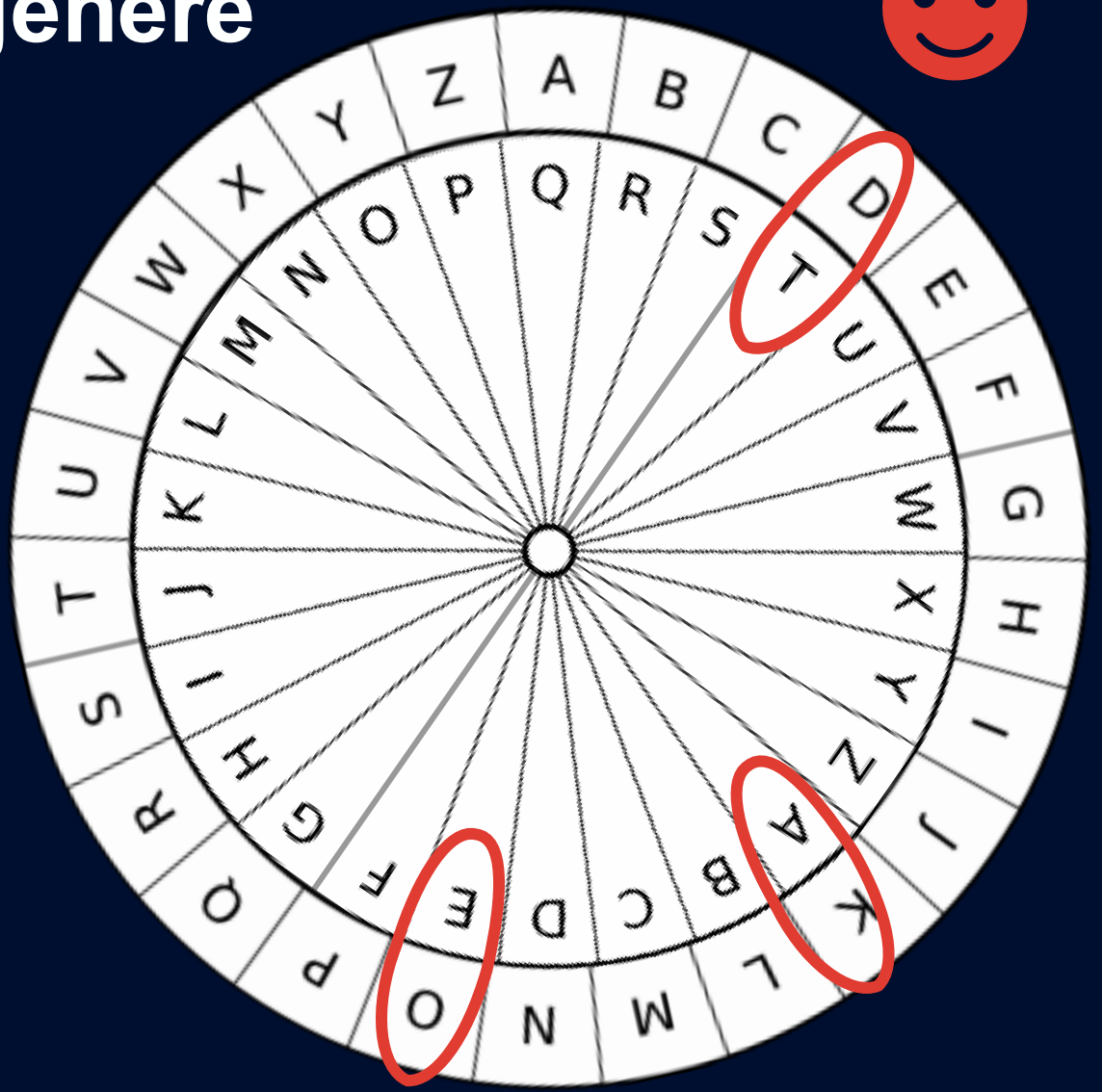
Frequency analysis -> Vigenère

1. We guess the length of the key is 3
2. We count the letters on the 1st 4th, 7th…. Spot
    1. Frequency O = 15 → E
    2. Frequency D = 11 → A,T?
    3. Frequency K = 11 --> A,T?



Frequency analysis -> Vigenère

1. We guess the length of the key is 3
2. We count the letters on the 1st 4th, 7th…. Spot
    1. Frequency O = 15 → E
    2. Frequency D = 11 → A,T?
    3. Frequency K = 11 --> A,T?



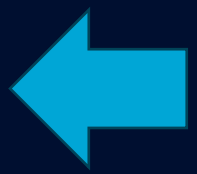
Frequency analysis -> Vigenère

1. We guess the length of the key is 3
2. We count the letters on the 1st 4th, 7th…. Spot
    1. Frequency O = 15 → E
    2. Frequency D = 11 → T
    3. Frequency K = 11 → A
3. Do the same for the 2nd and 3th letter of the key
4. Decrypt the message

xsu nyp sre dlg cxg wiq ref bex khf
khz yvl oog xkq ref bmw kvr rvc
owm xwm xxf oxf yyq krb krb pmp
cxl skf daf orq rif khc xhc nxf oxy
vim pqy kvs pwf ovm ciy xhi swq ohr
rie bss xhz ojm bif sqq kcg xke biy
dog xkd yvy dlm ewy xhy xhm xil skf
dwg ret ofc orp ogm err sre dsw yyr
rid kfj owm pty cxy qiq krb dlc vie
orb csd kra sil dog xkq wew sqy uiq
yfm vhy cxm mvy fiy pet yyp yjw yyp
weh owr iin spm qyc dej owd bsk
dlc dlm ewy xhy xhm xil skf dw

Frequency analysis -> Vigenère

Now during this time Shahrazad had borne king Shahriyar three sons. On the thousand and first night, when she had ended the tale of Ma'aruf, she rose and kissed the ground before him, saying: “great king, for a thousand and one nights I have been recounting to you the fables of past ages and the legends of ancient kings. May I make so bold as to crave a favour of your majesty?”
Epilogue, Tales from the Thousand and One Nights



xsu nyp sre dlg cxg wiq ref bex khf
khz yvl oog xkq ref bmw kvr rvc
owm xwm xxf oxf yyq krb krb pmp
cxl skf daf orq rif khc xhc nxf oxy
vim pqy kvs pwf ovm ciy xhi swq ohr
rie bss xhz ojm bif sqq kcg xke biy
dog xkd yvy dlm ewy xhy xhm xil skf
dwg ret ofc orp ogm err sre dsw yyr
rid kfj owm pty cxy qiq krb dlc vie
orb csd kra sil dog xkq wew sqy uiq
yfm vhy cxm mvy fiy pet yyp yjw yyp
weh owr iin spm qyc dej owd bsk
dlc dlm ewy xhy xhm xil skf dw

Real world example

Enigma | World war I and II

Explanation video Enigma:
https://www.youtube.com/watch?v=ybkkiGtJmkM

Movie of Alan Turing:

The Imitation Game

Invention of Enigma

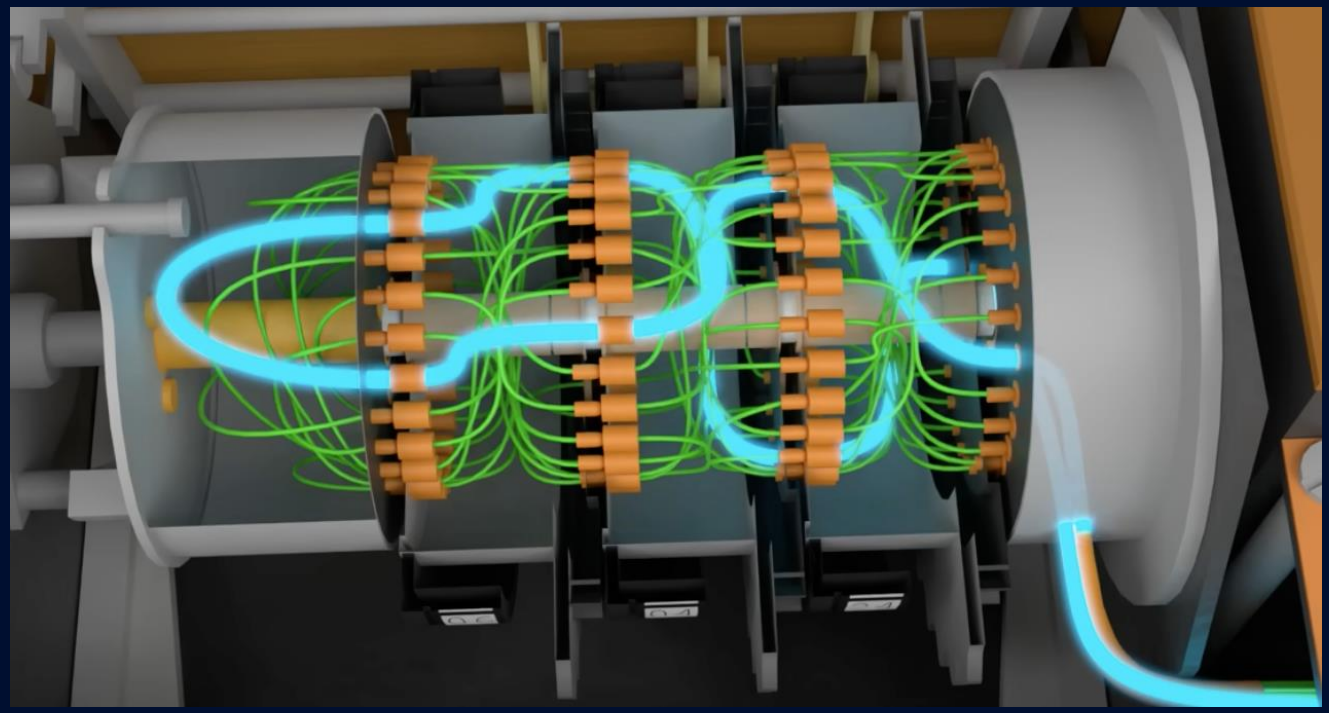
- In 1915
- By two Dutch for the Dutch War Ministry
- First prototype by the end of WW I

What is enigma

- Machine to encrypt/ decrypt
- Keyboard to type text
- Lightbulbs to see encrypted text
- Encryption mechanism
  - 3 wheels → encrypt letters

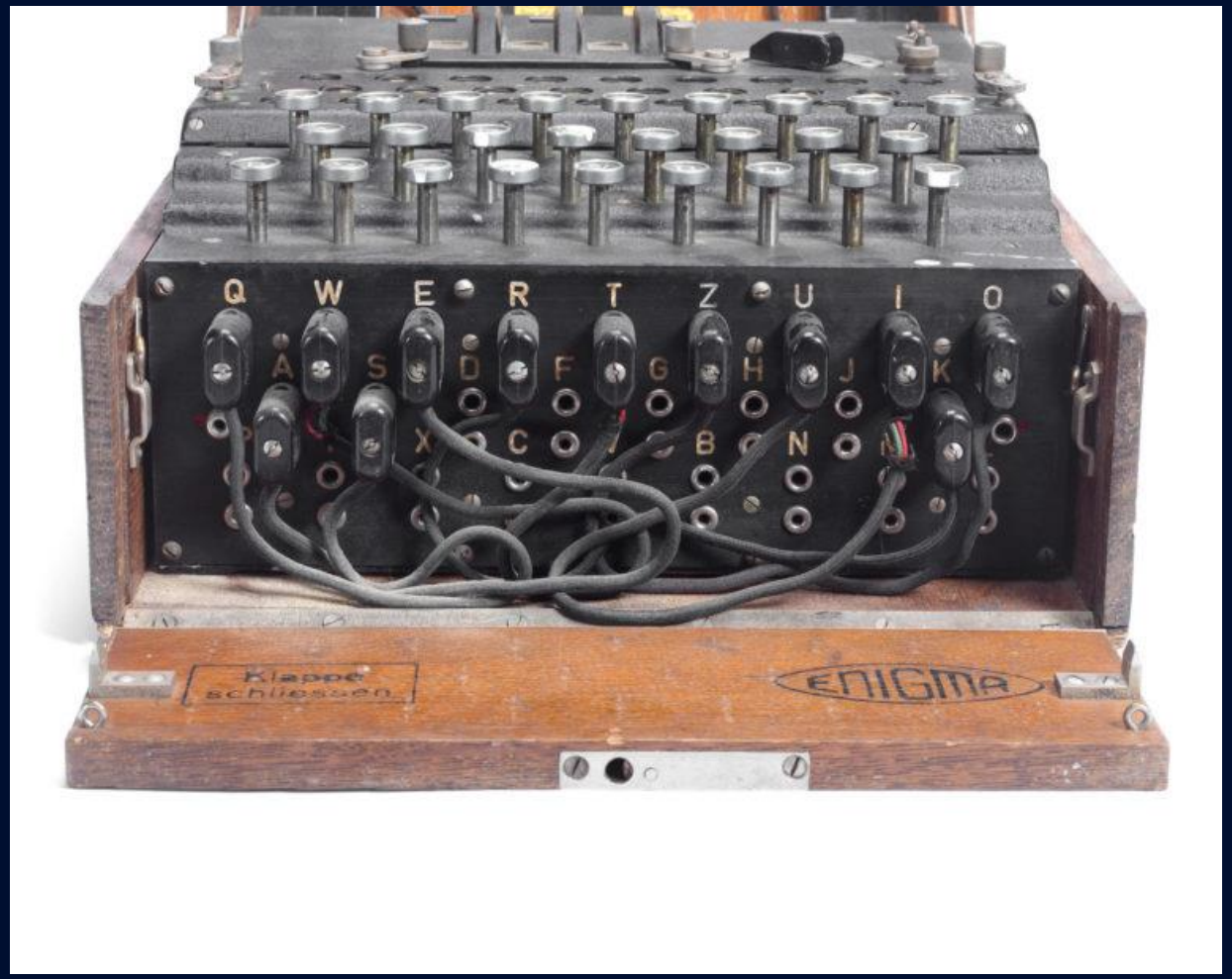
What is enigma

- Machine to encrypt/ decrypt
- Keyboard to type text
- Lightbulbs to see encrypted text
- Encryption mechanism
  - 3 wheels → encrypt letters
  - A lot of wires



What is enigma

- Machine to encrypt/ decrypt
- Keyboard to type text
- Lightbulbs to see encrypted text
- Encryption mechanism
  - 3 wheels → encrypt letters
  - A lot of wires
  - “Stecker” → swap letters



Encryption – Decryption with Enigma

- Encryption and decryption was done with the same machine
- But both machines need the same setting:
  - The orientation of the wheels
  - The “steckers” in the stecker board
- Distribute these settings via:
  - Sheets
  - Codebooks

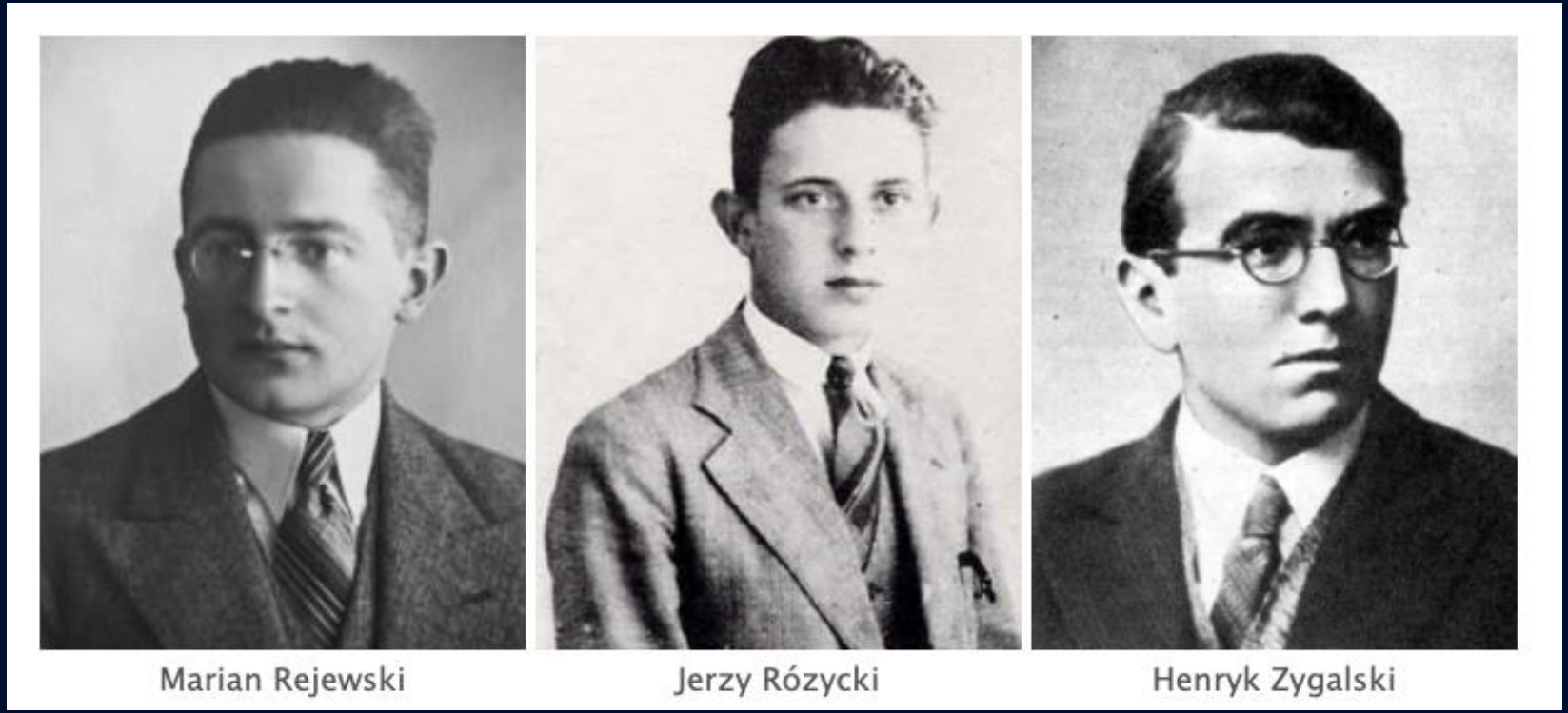
Evolution of Enigma

- Enigma A (1924) → 26 keys
- Enigma B (1924) → 28 keys
- Enigma C (1925) → 29 keys
- Enigma D (1926)

- Enigma K (1927) → Increased cipher strength
- Enigma I (1927-1929) → Exclusively used for military purposes

Military Enigma (Enigma I) Broken

- 3 Polish mathematicians broke Enigma I
- They needed around 100 intercepted messages to recover the initial settings



Stronger Enigma

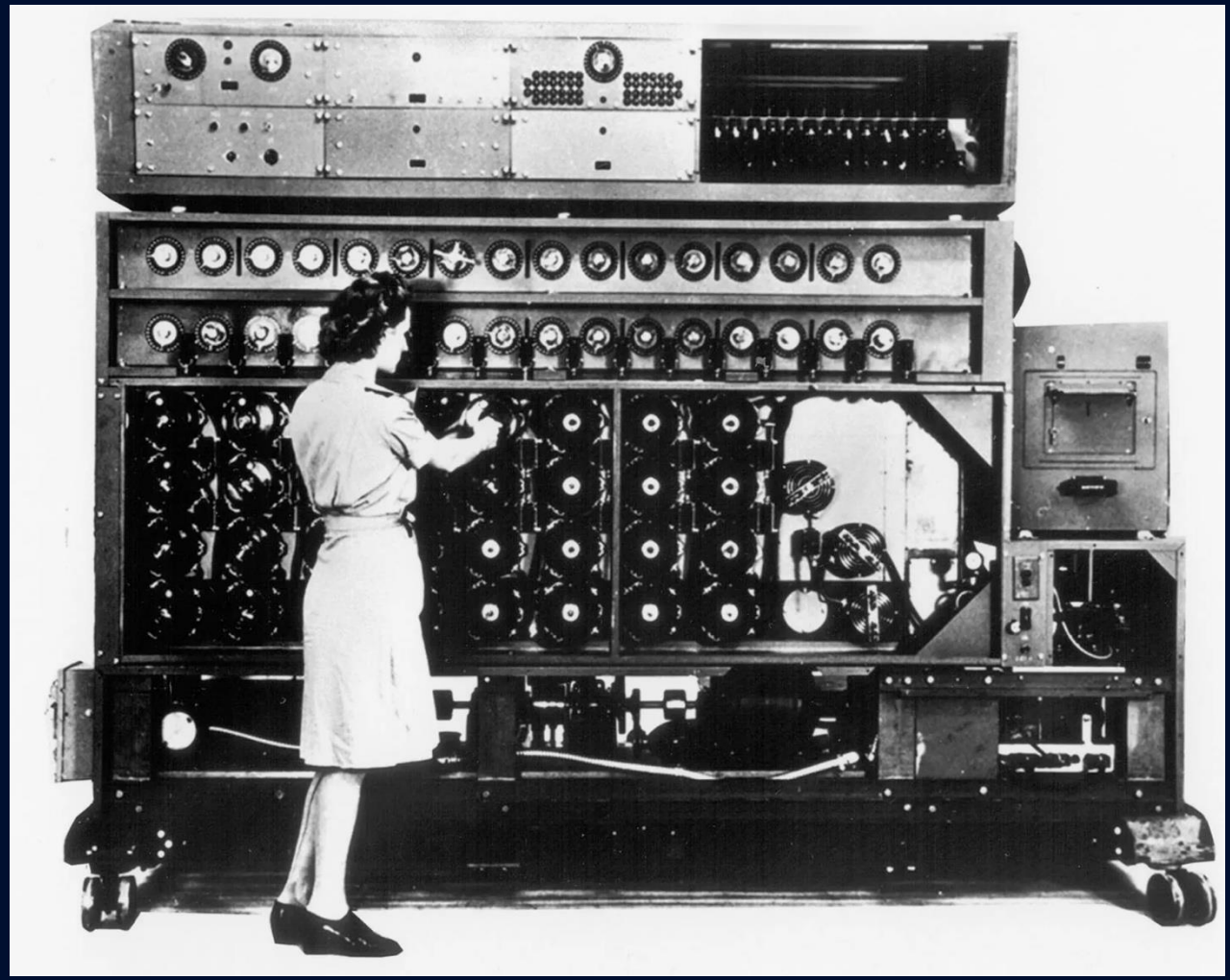
- Every enigma has an initial setting
  - 3 wheels
  - Stecker board
- Germans used only this setting
- But the Polish broke it with 100 messages… so…
- On 15 September 1938 the Germans had a new setting every day
- 2 wheels were added
  - 10 times more possible settings

Bletchley Park

- 45 miles north of London
- Since 14 August 1939 hosted Government Code and Cypher School
- Staff:
  - Professional code breakers
  - Chess players
  - Mathematicians
  - Organizers
- Among them: Alan Turing

Breaking Enigma

- Messages were broken by hand
- Alan Turing made the Bombe; a machine to break messages



New Enigma

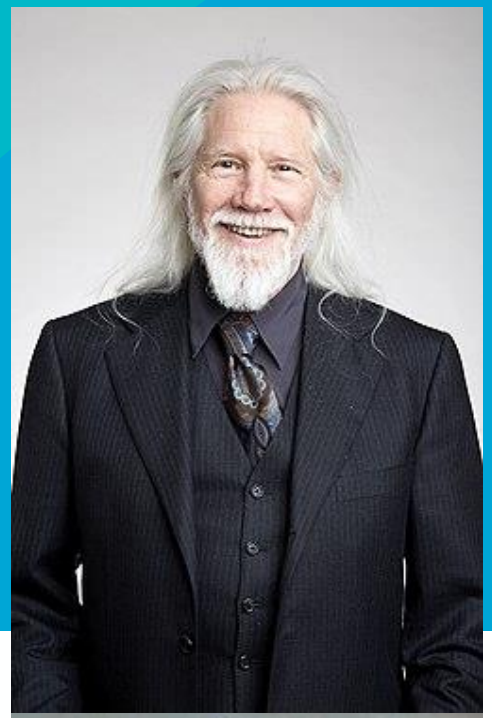
- On 1 February 1942, the German Navy introduced a new Enigma machine
- New wheel
- New indicator system
- New codebooks

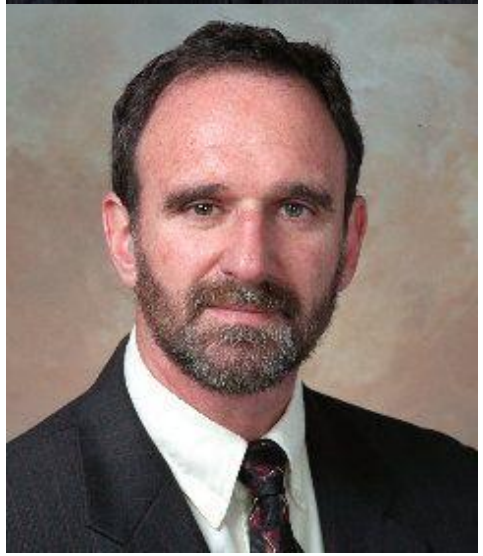
Breaking New Enigma

- Alan Turing discovered the new wiring
- They captured a new codebook 30 October 1942
- But Bombe was not suitable for breaking these machines
- The UK did not have enough resources to build a new machine
- The US had sufficient supplies and build the US Bombe

Why the Germans kept using Enigma

- Germany always believed that Enigma could not be broken
- The German Navy, however, had their doubt
  - The Navy thus introduced extra security measurements
- The German Air Force also added security
  - An extra device to be attached to Enigma
  - However, “due to operator mistakes it was broken within a few days after its introduction”
- Even after the war, it was kept secret that Enigma was broken



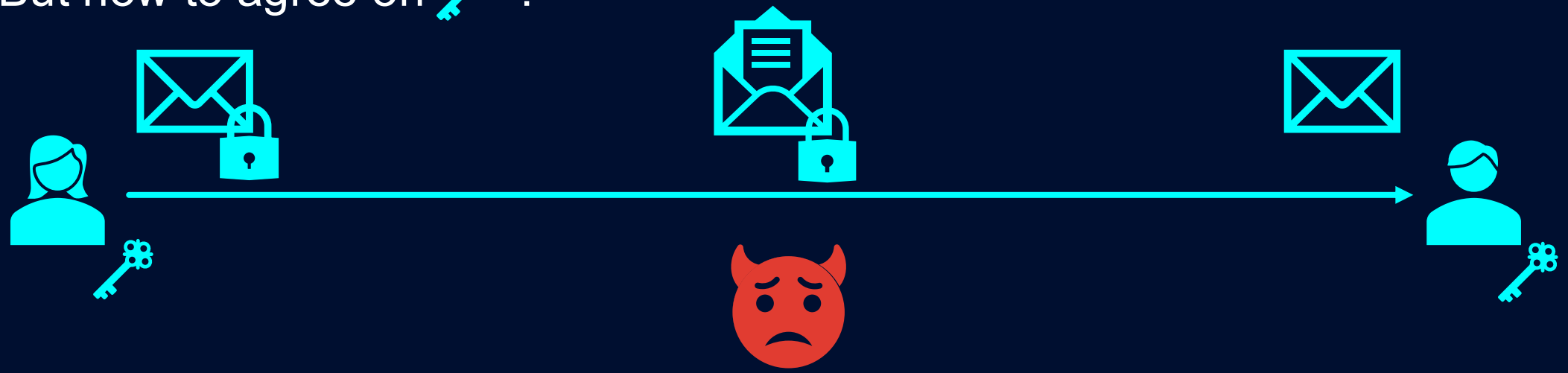


Diffie-Hellman

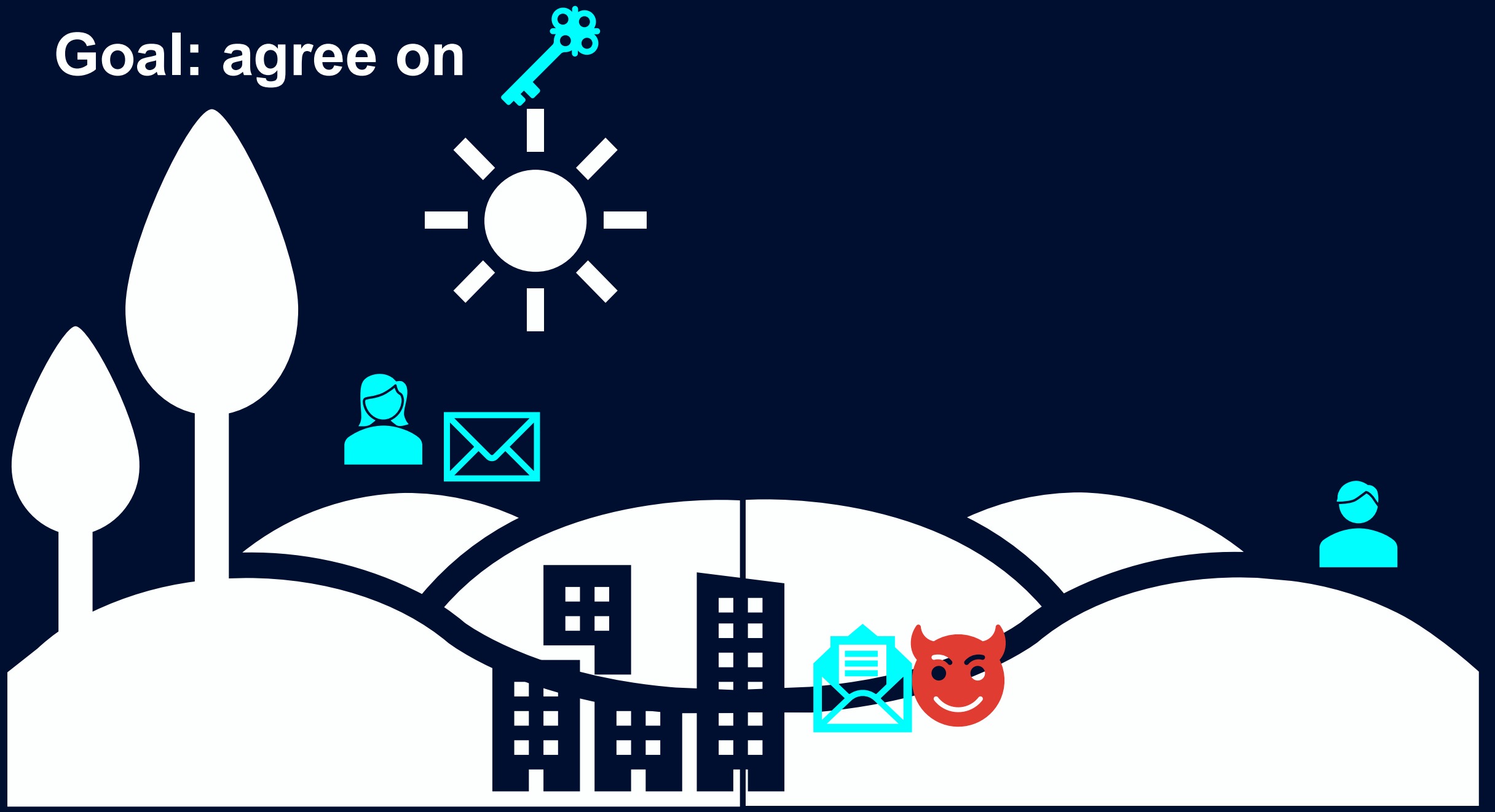
1976 – Building block of current cryptography

Recall: Goal of Alice

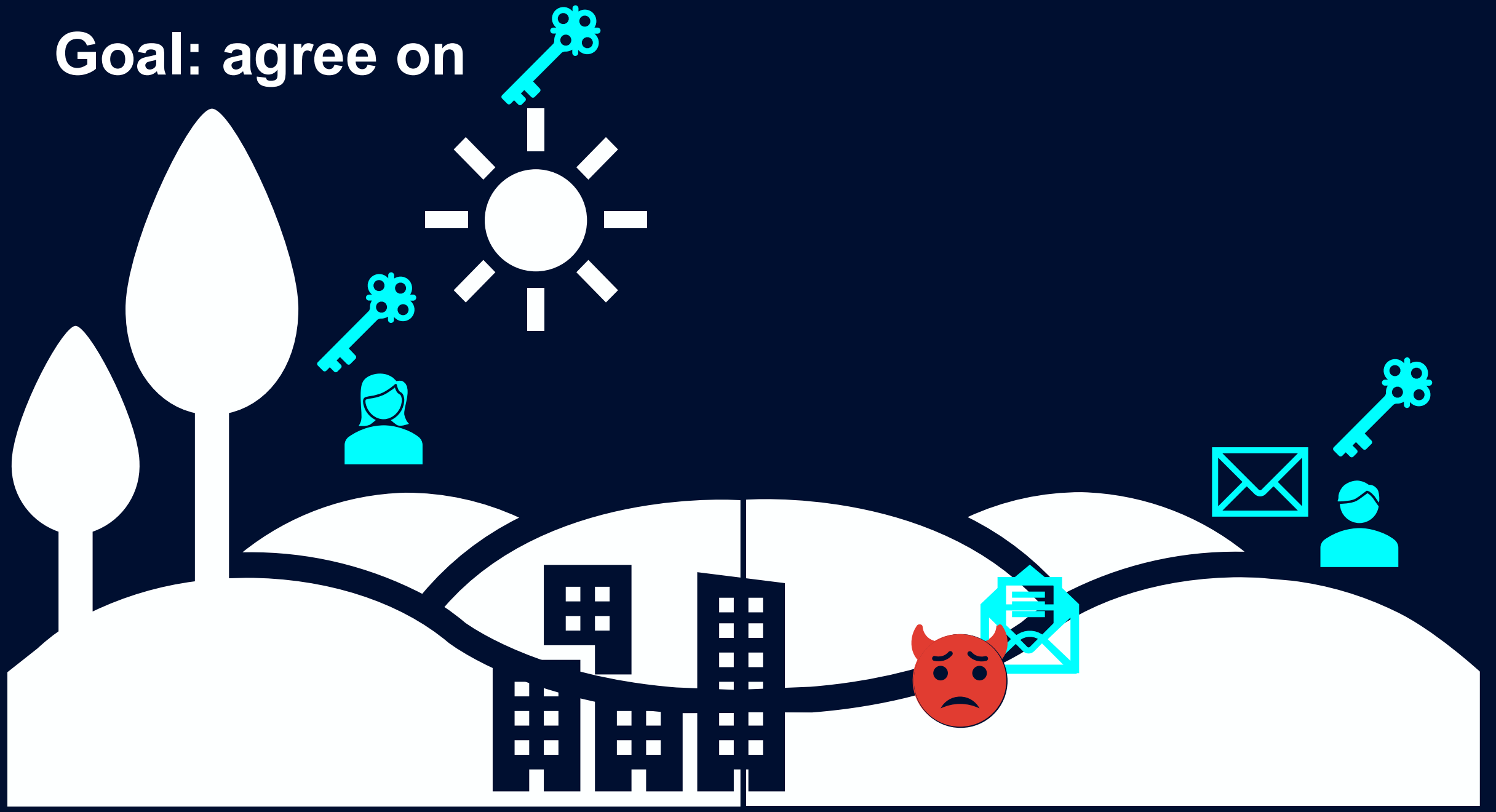
- A key that only Alice and Bob know
- Alice can *Encrypt* the message
- Bob can *Decrypt* the message
- If Eve sees the message, she will not understand
- But how to agree on ?



Goal: agree on



Goal: agree on



Diffie Hellman exchange

g (public parameter)

a = rand()
$A = g^a$

$A = g^a$

b = rand()
$B = g^b$

$B = g^b$

$K = B^a$

$K = A^b$

$K = g^{ab} = g^{ba}$

Diffie Hellman exchange

INSECURE

g (public parameter)

a = rand()
$A = g^a$

b = rand()
$B = g^b$

$A = g^a$

$B = g^b$

$K = B^a$

$K = A^b$

$a = log_g(A)$
$K = B^a$

“Normal” arithmetic

- Given $a,\ g$
- Easy to compute:

$$A \equiv g^a$$

- Given A, g
- Easy to compute:

$$a \equiv log_g(A)$$

Modular arithmetic

- Given $a,\ g,\ p$
- Easy to compute:

$$A \equiv g^a mod\ p$$

- Given A, g, p
- **Difficult** to compute:

$$a \equiv log_g(A) mod\ p$$

Diffie Hellman exchange

INSECURE

g (public parameter)

a = rand()
$A = g^a$

b = rand()
$B = g^b$

$K = B^a$

$K = A^b$

$K = g^{ab} = g^{ba}$

Diffie Hellman exchange

SECURE

g and p (public parameter)

a = rand()
$A = g^a \bmod p$

b = rand()
$B = g^b \bmod p$

$= B^a \bmod p$

$= A^b \bmod p$

$K = g^{ab} = g^{ba}$

Diffie Hellman exchange

SECURE

g and p (public parameter)

a = rand()
A = g^a mod p

b = rand()
B = g^b mod p

A = g^a

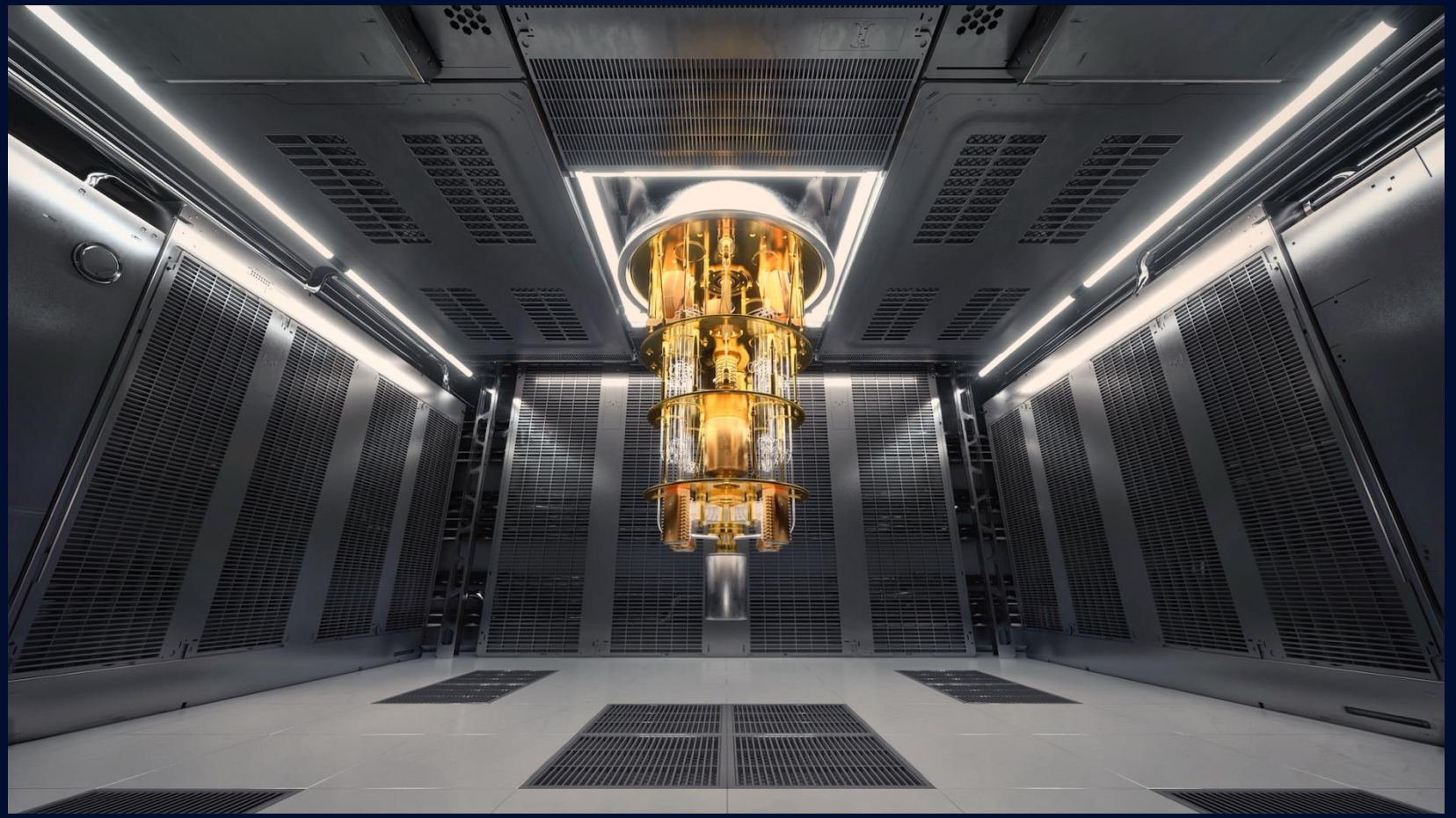
B = g^b

= B^a mod p

= A^b mod p

a = $log_g(A)$

Breaking Diffie-Hellman



Thanks for your attention!